WHAT IS CLAIMED IS:

1. A method of transporting a random block of bits in a quantum cryptographic key distribution (QKD) network, comprising:

sharing blocks of bits between nodes in a QKD network using quantum cryptographic mechanisms;

determining a key transport path between a source node and a destination node in the QKD network, wherein the key transport path comprises one or more intermediate nodes;

at each intermediate node of the one or more intermediate nodes, logically combining a block of secret bits shared with a previous hop along the path with a block of secret bits shared with a next hop along the path to produce first combined blocks of bits;

at the destination node, logically combining a block of secret bits shared with a previous hop along the path with a random block of bits to produce a second combined block of bits;

receiving the first combined blocks of bits and the second combined block of bits at the source node; and

logically combining, at the source node, the first combined blocks of bits and the second combined block of bits to determine the random block of bits.

2. The method of claim 1, further comprising:

using the random block of bits to encrypt data sent between the source node and the destination node.

3. The method of claim 1, wherein logically combining, at each intermediate node, the block of secret bits shared with the previous hop along the path with the block of secret bits shared with the next hop along the path comprises:

combining the secret block of bits shared with the previous hop with the block of secret bits shared with the next hop along the path using an associative, invertible mathematical function.

4. The method of claim 3, wherein logically combining, at the destination node, the block of secret bits shared with the previous hop along the path with the random block of bits further comprises:

combining the secret block of bits shared with the previous hop along the path with the random block of bits using the mathematical function.

5. The method of claim 4, wherein logically combining the first combined blocks of bits and the second combined block of bits comprises:

combining selected blocks of bits of the first combined blocks of bits and the second combined block of bits, using the mathematical function, to determine the random block of bits.

6. The method of claim 5, wherein the associative, invertible mathematical function comprises a logical exclusive OR.

7. A method of end-to-end transport of a secret key in a quantum cryptographic key distribution (QKD) network, comprising:

determining multiple paths for end-to-end transport, employing QKD techniques, of the secret key across a QKD network; and

transporting the secret key across each of the determined multiple paths.

8. The method of claim 7, wherein the multiple paths comprise multiple disjoint paths.

9. The method of claim 7, wherein the multiple paths comprise multiple, partially disjoint paths.

10. The method of claim 7, further comprising:

determining link metrics associated with quantum cryptographic links of the QKD network.

11. The method of claim 10, wherein determining the multiple paths for transporting the secret keys across the QKD network comprises:

determining the multiple paths based on the determined link metrics.

12. The method of claim 10, further comprising:

exchanging a respective number of secret key bits between each node of the QKD network using the QKD techniques.

13. The method of claim 12, wherein determining the link metrics associated with the quantum cryptographic links of the QKD network comprises:

determining the link metrics based on the respective number of secret key bits exchanged between each node of the QKD network.

14. A method of transporting a key between a first node at one end of a path through a quantum cryptographic key distribution (QKD) network to a second node at an opposite end of the path, the QKD network comprising a plurality of nodes, the method comprising:

transmitting secret bits between the plurality of nodes of the QKD network using quantum cryptographic mechanisms;

reserving, from the first node, portions of the transmitted secret bits at each intermediate node along the path between the first and the second node; and

transporting a key between the second node and the first node using the reserved portions of the transmitted secret bits.

15. The method of claim 14, wherein transmitting secret bits between the plurality of nodes further comprises:

transmitting different secret bits between different pairs of nodes of the plurality of nodes.

16. The method of claim 15, wherein reserving the portions further comprises:

reserving portions of the transmitted different secret bits between each pair of nodes of the different pairs of nodes.

17. The method of claim 14, further comprising:

sending the reserved portions of the transmitted key symbols to the first node.

18. The method of claim 14, further comprising:

sending a reservation message from the first node to each intermediate node along the path.

19. The method of claim 18, further comprising:

reserving a respective portion of the portions of the transmitted secret bits at each intermediate node in response to each reservation message.

20. The method of claim 19, further comprising:

receiving, at the first node, a respective portion of the portions of the transmitted secret bits from each intermediate node in response to each reservation message.

21. The method of claim 20, further comprising:

receiving, at the first node, a respective portion of the portions of the transmitted secret bits, logically combined with the key, from the second node.

22. The method of claim 21, further comprising:

determining, at the first node, the key using the respective portions of the transmitted secret bits received from the second node and each intermediate node.

23. A computer-readable medium containing instructions for controlling at least one processor to perform a method of transporting a key across a quantum cryptographic key distribution (QDK) network, the method comprising:

reserving portions of key symbols, transmitted between nodes in the QKD network via quantum cryptographic mechanisms, at each node along a path across the QKD network; and

using the reserved portions of the transmitted key symbols to determine an encryption key for encrypting data sent between nodes at either end of the path.

24. A node at a first end of a path in a quantum cryptographic key distribution (QKD) network, comprising:

processing logic configured to:

reserve portions of key symbols, transmitted between nodes in the QKD network via quantum cryptographic mechanisms, at each node along a path across the QKD network, and

one or more interfaces configured to:

receive the reserved portions of key symbols,

the processing logic further configured to:

use the reserved portions of the transmitted key symbols to determine an encryption key for encrypting data sent to another node at a second end of the path.

25. A method of employing blocks of secret bits in communicating between a source node and a destination node in a network, comprising:

transmitting the blocks of secret bits between each node along a path between the source node and the destination node using quantum cryptographic mechanisms, wherein a different block of secret bits of the blocks of secret bits is transmitted between each different link that connects each node along the path;

initiating a reservation process, at the source node, the reservation process reserving at least a portion of the blocks of secret bits at each node along a path between the source node and the destination node; and

employing the reserved blocks of secret bits in subsequent public communication between the source node and the destination node.

26. A system for transporting a key between a first node at one end of a path through a quantum cryptographic key distribution (QKD) network to a second node at an opposite end of the path, the QKD network comprising a plurality of nodes, comprising:

means for transmitting secret bits between the plurality of nodes of the QKD network using quantum cryptographic mechanisms;

means for reserving, from the first node, portions of the transmitted secret bits at each intermediate node along the path between the first and the second node; and

means for transporting a key between the second node and the first node using the reserved portions of the transmitted secret bits.

27. A method of sharing data with a first endpoint in a path between the first endpoint and a second endpoint in a quantum cryptographic network, comprising:

sharing a first block of data with a preceding neighboring node in the path using quantum cryptographic mechanisms;

sharing a second block of data with a subsequent neighboring node in the path using quantum cryptographic mechanisms;

logically combining the first and second block of bits to produce a result;

receiving a message from the first endpoint; and

sending the results to the first endpoint based on receipt of the message.

28. A relay node in a path between a first endpoint and a second endpoint in a quantum cryptographic network, comprising:

a quantum cryptographic transceiver configured to:

share a first block of data with a preceding neighboring node in the path using quantum cryptographic mechanisms, and

share a second block of data with a subsequent neighboring node in the path using quantum cryptographic mechanisms;

processing logic configured to:

logically combine the first and second block of bits to produce a result; and

an interface configured to:

receive a message from the first endpoint, and

send the results to the first endpoint based on receipt of the message.

29. A method of transporting a secret key along a portion of a path between a first quantum cryptographic endpoint and a second quantum cryptographic endpoint in a quantum cryptographic system, comprising:

sharing a first block of data with a neighboring node in the path between the first quantum cryptographic endpoint and the second cryptographic endpoint using quantum cryptographic mechanisms;

receiving a second block of data from the neighboring node, wherein the second block of data comprises a secret key logically combined with the first block of data; and

logically combining the second block of data with the first block of data to recover the secret key.

30. The method of claim 29, wherein the second block of data comprises a secret key exclusively ORed with the first block of data.

31. The method of claim 30, wherein the logically combining comprises:

exclusively ORing the second block of data with the first block of data to recover the secret key.

32. A relay node in a path between a first endpoint and a second endpoint in a quantum cryptographic system, comprising:

a quantum cryptographic transceiver configured to:

share a first block of data, using quantum cryptographic mechanisms, with a neighboring node in the path between the first endpoint and the second endpoint;

an interface configured to:

receive a second block of data from the neighboring node, wherein the second block of data comprises a secret key logically combined with the first block of data; and

processing logic configured to:

logically combine the second block of data with the first block of data to recover the secret key.